



November 2, 2021

NOTICE OF EX PARTE

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Womble Bond Dickinson (US) LLP

2001 K Street, NW
Suite 400 South
Washington, DC 20006

t: 202.467.6900
f: 202.467.6910

Re: Promoting the Deployment of 5G Open Radio Access Networks, GN Docket No. 21-63; Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, WC Docket No. 18-89

Caressa D. Bennet
Partner
Direct Dial: 202-857-4519
Direct Fax: 202-261-0079
E-mail: Carri.Bennet@wbd-us.com

Dear Ms. Dortch,

On October 29, 2021, John Baker, SVP, Business Development of Mavenir Systems, Inc. ("Mavenir"); Maryvonne Tubb, Mavenir SVP, Global Marketing & Communications; Loris Zaia, Mavenir VP, Major Accounts; Caressa Bennet and E. Alex Espinoza, counsel for Mavenir Systems, Inc. (collectively, "Mavenir"), met via video conference with Nicholas Copeland, Patrick DeGraba, Cher Li, Catherine Mataves, Mark Montañó, Don Stockdale, and Patrick Sun, from the Office of Economics and Analytics; Charles Matthias, and Kambiz Rahnnavardy from the Wireless Telecommunications Bureau; Martin Doczkat and Sean Yun from the Office of Engineering and Technology; and Justin Faulb, from the Wireline Competition Bureau (collectively, "FCC Staff"). Mavenir and FCC Staff discussed the following issues in the above-captioned dockets:

Open RAN

Deployment status. FCC Staff inquired as to Open RAN's domestic and international deployment status. Mavenir has multiple trials and commercial deployments with carriers worldwide currently underway, notably with Dish (U.S.); Deutsche Telekom, O-RAN Town (Germany); Vodafone (U.K.); Axiata (Malaysia); Triangle (U.S., Supply Chain Reimbursement Program); and TIM (Italy). FCC Staff noted docket commenters claim that Open RAN is only deployable in certain environments, *i.e., greenfield not brownfield*.¹ With respect to Open RAN deployment, Mavenir stressed that terms like brownfield and greenfield are misnomers;² an apparent marketing ploy, presumably to create the misimpression that Open RAN is only deployed or deployable in certain locations or environments. Mavenir clarified that Open RAN is deployable anywhere, regardless of whether the network was established years ago, or is yet to be stood up. What matters is open interfaces for interoperability.

¹ See TechTarget, *greenfield deployment*, <https://searchunifiedcommunications.techtarget.com/definition/greenfield-deployment> (last visited Oct. 29, 2021) ("In networking, a greenfield deployment is the installation and configuration of a network where none existed before, for example in a new office. A brownfield deployment, in contrast, is an upgrade or addition to an existing network and uses some legacy components. The terms come from the building industry, where undeveloped land (and especially unpolluted land) is described as *greenfield* and previously developed (often polluted and abandoned) land is described as *brownfield*.").

² See *generally* John Baker, Mavenir, Open RAN – Clearing up Confusion About Greenfield and Brownfield References (2021) (Attached to this notice of ex parte as Attachment 1).



To ensure interoperability, standard-setting bodies such as 3GPP should freely open interfaces—e.g., the X2 family of interfaces, which are designed for *interoperability*—and not use them instead for vendor commercial advantage.

Market failure. FCC Staff asked Mavenir whether the present status quo represents a market failure—in economic terms—of the Radio Access Network (“RAN”) market, to which Mavenir emphatically agreed. As the Commission has previously written, in economic terms, one market failure involves *market power*, where barriers to entry only allow one or a small number of firms to serve a market.³ These firms are said to have *market power*, and are called “dominant providers.”⁴ “Classic regulatory responses to market power include regulating the prices or output of a monopolized industry, such as a water, electricity or telephone service. Or the regulator might break up a monopoly and introduce competition.”⁵ In one notable example, the FCC responded to wireless carrier market power to reduce cell phone locking “which tied consumers for long periods to one wireless service provider,”⁶ by warning the wireless industry it should voluntarily unlock handsets, before the Commission acted via regulation. Upon threat of Commission action, the wireless industry voluntarily permitted subscribers to unlock their phones and use them with a different wireless service provider.

Here, similarly, the Commission should also make the incumbent providers open their radio interfaces. The incumbent providers—Ericsson, Nokia, and Huawei—are all foreign-headquartered companies that have monopolized the existing RAN market, and appear to be using that existing dominant market power to dominate the new and emerging 5G RAN market.⁷ Wireless carriers are currently locked to one vendor per chosen solution, *i.e.*, “vendor lock”: Carriers choosing equipment from any of the incumbent providers in the U.S. must purchase *all* equipment and associated services from that company, due to the proprietary nature of the provider’s RAN equipment.⁸ This would be akin to Dell only allowing the use of Dell software and peripherals on Dell computers, and forcing those customers to use Dell software and hardware indefinitely. Given the national security implications of securing our wireless

³ See Public Safety and Homeland Security Bureau, FCC, FCC White Paper - Cybersecurity Risk Reduction at 44 (2017), <https://docs.fcc.gov/public/attachments/DOC-343096A1.pdf>.

⁴ *Id.* at 44. “Market power refers to the ability of a firm (or group of firms) to raise and maintain price above the level that would prevail under competition. The exercise of market power leads to reduced output and loss of economic welfare.” *Id.* citing OECD, Glossary of Statistical Terms – Market Power, <https://stats.oecd.org/glossary/detail.asp?ID=3256> (last visited Oct. 29, 2021)).

⁵ Public Safety and Homeland Security Bureau, FCC, FCC White Paper - Cybersecurity Risk Reduction at 44 (2017), <https://docs.fcc.gov/public/attachments/DOC-343096A1.pdf>.

⁶ *Id.* at 45.

⁷ Ericsson is headquartered in Sweden; Nokia in Finland; and Huawei in China. See Ericsson, *Ericsson in Sweden*, <https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/sweden> (last visited Nov. 1, 2021) (“Our headquarters are located in Stockholm, Sweden, which has been our base for the past 140 years”); Nokia, *Contact Us*, <https://www.nokia.com/contact-us/> (last visited Nov. 1, 2021); Uptin Saiidi, *Take a look around Huawei’s headquarters in China*, CNBC (May 10, 2018, 4:53AM EDT), <https://www.cnbc.com/2018/05/10/inside-huawei-headquarters-in-shenzhen-china.html>.

⁸ See Letter from Tom Wheeler, Chairman, FCC, to Steve Largent, President and CEO, CTIA – The Wireless Association (Nov. 14, 2013), <http://cdn0.sbnation.com/assets/3571903/CTIA111413.pdf>; CTIA, *Wireless Industry Commitment – Consumer Code for Wireless Service*, <https://www.ctia.org/the-wireless-industry/industry-commitments/consumer-code-for-wireless-service> (last visited Oct. 29, 2021) (stating “Mobile wireless device unlocking . . . a device that works on one carrier’s network may not be technologically compatible with another carrier’s network.”).



networks, the FCC should initiate a rulemaking to impose a policy for open interfaces, as opposed to a strongly worded letter. Mavenir reiterates that this is not a technological change, only a policy change to open interfaces and allow interoperability, which will provide operators the freedom to use *any* vendor, or keep existing vendors.

Open RAN cost savings. Open RAN will allow for cost savings over proprietary architectures. Mavenir walked the attendees through the 40% Operational Expenditure (OpEx) and 36% Total Cost of Ownership (TCO) cost savings for Open RAN, as itemized in the newly corrected Cost Catalog.⁹ All size carriers, including small carriers, will be able to map and right-size their networks in terms of expenditures and maintenance.

Security and interoperability. Mavenir answered questions on Open RAN's security and interoperability benefits, and specifically addressed recent stories in the telecom trade press claiming Open RAN must first be secure "to be accepted." Mavenir stated that any RAN architecture, open or closed, must be secure. What is disingenuous is to suggest that Open RAN is unsecure. On the contrary, Open RAN's Zero Trust philosophy ensures every component in the RAN is secure from the start. Open interfaces mean that wireless carriers can pick the components that work best for them, and seamlessly integrate them in secure networks.¹⁰ Mavenir also noted that the incumbent equipment providers are continuing to propose proprietary, virtualized interfaces, which are untested by outside parties, and may accordingly have unknown security vulnerabilities that their wireless carrier customers are not able to determine or address.

Use of legacy and 4G/5G by small providers. FCC Staff inquired as to whether Open RAN could assist small and rural providers to simultaneously operate legacy 2G/3G networks and newer 5G networks. Mavenir noted that all size carriers opting to keep legacy 2G and 3G networks operating during those networks' pending sunset, and combine 4G/5G networks (and beyond) can do so.

Domination of standards' setting bodies by incumbents and Huawei. Mavenir and FCC Staff discussed the present domination of standards' setting bodies by Ericsson, Nokia, and Huawei. As discussed in Mavenir's previous *ex parte* filing, by allowing closed infrastructure to be used for the Supply Chain Reimbursement Program, the Commission is implicitly supporting closed proprietary interfaces derived through the CPRI Cooperation, a small, exclusionary, non-public, technical group, which keeps full specification detail confidential and limited to those incumbent manufacturers, including Huawei. This group continues to set proprietary standards, specifically for the CPRI and eCPRI standards.¹¹ Allowing Ericsson, Nokia and NEC to collaborate with Huawei, a Covered List company,¹² to continue to develop closed propriety standards for 5G is unfathomable.

⁹ See Attachment 2, below, included as requested by FCC Staff.

¹⁰ Mavenir has attached its security overview to this notice of *ex parte*, included here as Attachment 3, as requested by FCC Staff. Mavenir's white paper, *Security in Open RAN*, is also included as Attachment 4, below.

¹¹ See *CPRI Cooperation - Common Public Radio Interface*, <http://cpri.info/contact.html> (last visited Nov. 2, 2021) (showing exclusive cooperation by Ericsson, Huawei, NEC, and Nokia).

¹² Covered list companies are those the FCC designates as producing "communications equipment and services (Covered List) that are deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons." FCC, *List of Equipment and Services Covered By Section 2 of The*



Virtualization/AI/machine learning. With respect to virtualization, AI, and machine learning, Mavenir discussed that any vendor can step in and provide these services with Open RAN architecture.

Power performance and efficiency. FCC staff inquired about Mavenir's claims on Open RAN's power performance and efficiency, and how that translated into customer cost savings. Mavenir provided an overview of Open RAN's cost savings and power efficiencies, which information is attached to this notice of ex parte.¹³

Supply Chain

FCC Staff inquired about the concerns small carriers have recently voiced about the nationwide carriers' Open RAN adoption status. Mavenir stressed that small carriers have legitimate reason for concern; vendor lock-out is keeping the nationwide carriers from adopting Open RAN, and is in turn keeping smaller carriers from adopting Open RAN. If the Commission were to require all vendors to open RAN interfaces, both nationwide carriers and small carriers would be able to deploy Open RAN into their existing networks. It is critical that the Commission act on an Open RAN rulemaking, as Reimbursement Program applicants are making critical decisions now as part of the FCC's Reimbursement Program application filing window which opened October 29, 2021 and is scheduled to close January 14, 2021.¹⁴

With respect to the Cost Catalog and Reimbursement Program guidelines, Mavenir stressed that the rules will have the effect of favoring high-cost proprietary equipment vendors, over those of lower cost vendors, including Open RAN vendors. The Commission's Third Report and Order articulated that in the event currently available funding is insufficient to meet Reimbursement Program funding needs, the Commission will prorate funding across all requests, commensurate with the funding shortfall.¹⁵

Because the Commission will apportion applicant funding using Cost Catalog line item average costs, Mavenir stressed to FCC Staff that Reimbursement Program applicants initially opting for lower cost Open RAN equipment and services should not have their funding reduced because they started off with the more secure and cost effective solution. Those choosing the higher cost option have an option to go to the lower cost solutions if they wish, whereas those choosing the lower cost Open RAN solution initially are penalized and do not have another lower cost option apart from self-funding the difference.

The Commission should incentivize wireless carriers to adopt U.S. technologies and vendors by *fully funding* Open RAN for the Reimbursement Program. The only way to prevent another Rip and Replace is to ensure wireless providers use vetted, secure equipment and services. While the FCC should continue to be technology neutral, it should not be cost neutral. The

Secure Networks Act, <https://www.fcc.gov/supplychain/coveredlist> (last visited Nov. 1, 2021). The Commission designated Huawei a Covered List company on March 12, 2021. *Id.*

¹³ See Attachment 5, below.

¹⁴ Press Release, FCC, FCC Opens Filing Window for Supply Chain Reimbursement Program (Oct. 29, 2021), <https://docs.fcc.gov/public/attachments/DOC-377383A1.pdf>.

¹⁵ See, e.g., *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Third Report and Order, FCC 21-86, at 27, para. 60 (Jul. 14, 2021).



Commission can choose to equip our U.S. networks with the secure, domestic cost-effective solution *now*—Open RAN.

Respectfully submitted,

/s/ Caressa D. Bennet
Caressa D. Bennet
E. Alex Espinoza
Womble Bond Dickinson (US) LLP
Counsel for Mavenir Systems, Inc.

Cc: Patrick DeGraba
Cher Li
Catherine Mataves
Mark Montañó
Don Stockdale
Patrick Sun
Nicholas Copeland
Martin Doczkat
Charles Matthias
Kambiz Rahnavardy
Sean Yun
Justin Faulb

Attachments (5)

ATTACHMENT 1

John Baker, Mavenir, *Open RAN – Clearing Up Confusion About Greenfield and Brownfield References*



Open RAN

CLEARING UP CONFUSION ABOUT GREENFIELD AND
BROWNFIELD REFERENCES

JOHN BAKER, SVP MAVENIR



Competitive Positioning of Open RAN feature capability being colored to add confusion

The terms “greenfield” and “brownfield” are being used to try to competitively differentiate the virtual distributed unit (vDU) software performance and capability of a vendor- and operator-deployed Open vRAN solution. “Greenfield” refers to a low-capacity network and “Brownfield” refers to a high-capacity network. Contrary to the narrative, the vDU’s that are available today support high-capacity features of 4G/5G, such as Carrier Aggregation, CoMP and interference coordination, for both greenfield and brownfield deployment.

A short history lesson

Since the birth of GSM back in the 90’s, all generations (2G, 3G, 4G and 5G) of mobile networks’ RAN(Radio Access Network) infrastructure interfaces have remained proprietary to the providing vendor. Apart from solutions being provided with “Open RAN” interfaces, this statement remains true today. 3GPP has specified the X2/Xn interface to allow gnb to gnb connectivity, but instead, legacy vendors used this interface as a commercial obstacle, prohibiting mixing of vendor RAN solutions.

As a result, today you cannot overbuild or mix and match proprietary vendor RAN solutions. Regrettably, all the features that are mentioned above, such as Carrier Aggregation and COMP, are proprietary solutions and are vendor specific. Because of the specific nature of these features, interworking between different vendor Open RAN and proprietary RAN solutions is currently not possible.

Advanced vDU features

Advanced vDU features, such as carrier aggregation, CoMP and Interference coordination, are possible and available today on vDU offerings. Sadly, these are still vendor specific solutions because 3GPP allowed propriety implementations. These features need focus by the O-RAN Alliance to schedule open specification of these parameters.

Today, vDU solutions are being tested under load for capacity and performance. System test, performance and stability are also being tested. As part of these tests:

- Call model scenarios are run to stress systems with a number of users and for long duration



- Number of users are loaded based on scenario and customer configuration. The typical common configuration used in lab tests are:
 - 100 Active users, 200 connected users per cell
 - 200 active users and 320 connected users per cell
 - Duration of test varies for each scenario. We aim to achieve 24hr+ stability with loaded scenarios at least.
- At the end of each long execution, KPIs are monitored and compared for performance assessments
- Open vRAN performance is shown to be equal to and in some cases, exceed that of existing incumbent vendors. [Reference: July FCC Open RAN Showcase – Mavenir presentation]

Open vRAN networks will support advanced features

The Open RAN industry will add advanced features, and vendors will compete on differentiated vDU solutions. We can expect the O-RAN Alliance and other organizations to standardize interfaces that enable more advanced features in an open environment, and companies like Intel, Mavenir and others are doing great work to implement advanced vDU features on standard server hardware. Operators will be able to upgrade software and processor technology for more capacity and features as they add customers like a Tesla customer boosting the performance of their car with a software upgrade.

Vodafone, Intel and Cohere have also demonstrated advanced features that are not available from proprietary RAN providers improving spectral efficiency.¹

Summary

- 1) vDUs support and will continue to support improved capacity and spectrum optimization features
- 2) Further specification work from the O-RAN Alliance and 3GPP needs to continue to specify common RF optimization and high-capacity features to include Carrier Aggregation and Comp.
- 3) To date, NO RAN network has been built as a multi-vendor, multi-featured network due to proprietary interfaces and algorithms.
- 4) The use of “greenfield”, “brownfield” are used for marketing purposes, adding confusion to the marketplace.

¹ <https://www.fiercewireless.com/tech/vodafone-boosts-5g-capacity-open-ran-demo>

ATTACHMENT 2

Open RAN Costs and Savings

Open RAN Savings - 36% TCO savings (Avg)

FCC Layer	LOW PRICE	HIGH PRICE	AVG PRICE	Nokia Example	Mavenir Example
	Proprietary	Proprietary	Proprietary	Proprietary	Open RAN
Access Layer	\$100	\$159	\$129	\$125	\$125
Distribution Layer - 50 eNodeBs	\$4,461	\$8,288	\$6,375	\$4,762	\$1,507
Distribution Layer - Site Material	\$1,535	\$4,888	\$3,211	\$2,600	\$905
Core Layer - EPC	\$1,347	\$2,776	\$2,062	\$2,000	\$1,347
Core Layer IMS	\$2,174	\$3,404	\$2,789	\$2,500	\$2,174
Software Layer - EMS/RAN licensing	\$900	\$2,160	\$1,530	\$1,050	\$0
Services Layer - Per Site deployment	\$6,118	\$14,016	\$10,067	\$6,966	\$4,650
Services Layer - Miscellaneous	\$408	\$1,009	\$709	\$595	\$408

Pricing from Widelity Report and Preliminary Cost Catalog (3/25/21) with 40% difference on Open RAN Correction
Columns 1 thru 5 Data provided by Nokia at RWA conference Dallas (6/30/2021)

Total	\$17,043	\$36,700	\$26,872	\$20,598	\$11,116
Annual Support/Maintenance	\$399	\$719	\$559	\$470	\$275
7% RAN, 10% Core					
5 Year total	\$1,993	\$3,594	\$2,794	\$2,350	\$1,373
Total CAPEX + OPEX	\$19,036	\$40,294	\$29,666	\$22,948	\$12,489
Open RAN Savings	\$6,547				\$10,459
	34%				46%

Open RAN Cost Per Site

Assumes 50 Site Cluster (~\$1.39M)

> Widelity Catalog

- Price shown is per site

Final Catalog of Eligible Expenses and Estimated Costs		Range of Estimated Costs		Costs
Index	Description	Low	High	Average
2.31.0	Open vRAN eNodeB Model is based on single band 50 site cluster. It includes RRU (Remote Radio Unit)/CU (Control Unit)/DU (Distributed Unit)/SW (Software)/NFVi (Network Functions Virtualization infrastructure). SW include all features, power licenses, and optional features.			
2.31.1	B71 (3 sector site) or B5 (3 sector) One RRU Type	27,016.00	64,838.00	45,927.00

> Mavenir Contents or Widelity Index 2.31.1

Description	Quantity
RADIO SITE (50)	
- RRU – Mavenir RRU, 2X40W, LTE BAND-71	150
- ORAN Distributed Unit (DU) Server (2.33.3) - ME1210 platform: CPU Xeon D-2187NT 16C/2.0GHz	50
- LTE Open RAN eNB SW Fee (4.2.13) - 4G RAN CU/DU License	50
- Open RAN Mgmt System (4.2.15) - mCMS SW Licenses (mCMS + VNFM/CNFM + CDM)	50
DATA CENTER (1)	
- Control Unit (CU) Server (2.34.2) - Dell PowerEdge R740 XL 2x 26c 512GB	3
- NFV Server (3.5.3) - Dell PowerEdge R740-8c 128GB - Control Node	1

ATTACHMENT 3

Mavenir Security Program Overview



Mavenir Security Program Overview

Date: 1-Nov-2021

Copyright © Mavenir 2021

1 Mavenir Cybersecurity Policy and Program

1.1 Cybersecurity Policy

Mavenir's Cybersecurity policy is to provide products and services which comply with industry and regulatory security standards, and which utilize best in class security strategies, technologies and processes. We protect the confidentiality, integrity and availability of data and information assets, including those entrusted to us by our customers, partners and suppliers.

1.2 Program Overview

Cybersecurity spans the Mavenir Product Life Cycle from inception through end of life. Mavenir implements policies and processes in all key functions including engineering, operations, and supply chain and management. Processes are in place to manage vulnerabilities, assess risk, mitigate and resolve issues and prevent malicious code in Mavenir and third party components. Data security is a primary focus, including compliance with GDPR and similar data protection requirements.

Mavenir's Product Security leader is responsible for administration and communication of Mavenir's Security Policy and processes.

Mavenir is TL9000 and ISO9001 certified across the organization, including security requirements from these standards. We are ISO27001 certified for Cloud services and integrate the ISO27001 requirements across our organization and products.

Mavenir's security framework and policies are developed in accordance with industry best practice, with guidance from recognized sources including ISO 27001, SANS, CERT, ISF and ISO15408/Common Criteria (CC).

The recently defined Network Equipment Security Assurance Scheme (NESAS) jointly defined by 3GPP and GSMA provides a consistent framework and common external audit program for multiple vendors and operators. Mavenir plans to achieve formal NESAS certification of our policies and processes in 4Q2021.

Product security requirements are driven by standards from 3GPP, ETSI, ITU, IETF, GSMA and other organizations, national regulations and customer requirements. Mavenir's Security Benchmarks are based on these standards, and guidelines including DISA STIG, CIS Benchmark and OWASP. We actively participate with standard bodies including GSMA, ETSI, 3GPP and ORAN.

A key aspect of Mavenir's overall cybersecurity program is our focus on ensuring a secure supply chain. This includes the inherent risk from dependence on a single vendor. Open and interoperable interfaces make networks more secure because they facilitate network threat identification with multiple suppliers implementing the common interfaces. Open interfaces also reduce overall product lifecycle cost and development duration by facilitating standard third-party test suites and opens a global market for multiple accredited test labs. Also, as and when a vulnerability is identified any element found to be a security risk can more easily be substituted out without the need for expensive, more wholesale change.

Periodic internal audits measure process adherence and effectiveness and drive process improvements. External audits ensure ongoing certification.

The CSO oversees the Mavenir Security Board, which is responsible for implementing and managing the Product Security Management Process. Security Board members include senior representatives from PLM, Engineering and Operations.

The Security Board facilitates communication using a publicly visible email address for input. The email address may be used by Mavenir staff, customers, vendors and suppliers to communicate security alerts, raise concerns, and otherwise communicate with the Security Board.

The email address is: security@mavenir.com

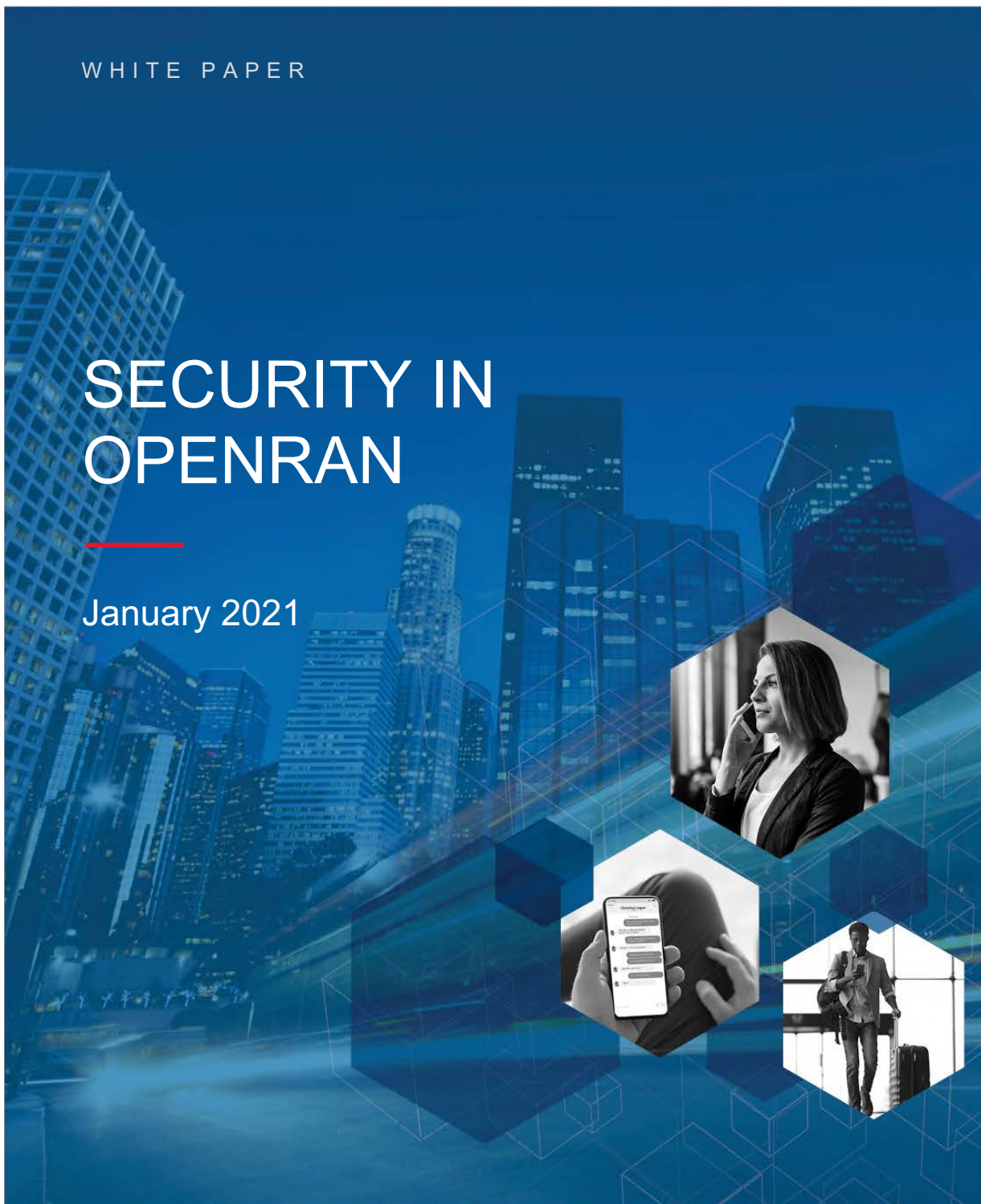
ATTACHMENT 4

Mavenir, *Security in Open RAN*

WHITE PAPER

SECURITY IN OPENRAN

January 2021



ALTIOSTAR

FUJITSU



mavenir.com

Table of Contents

1. Overview	4
2. Next Generation RAN Architectures	5
3. Open RAN security based on Zero Trust Architecture	7
4. Secured communication between Network Functions	8
4.1 Secure communication on all interfaces	8
4.2 Establishing trust based on mutual authentication	9
4.3 Trusted Certificate Authorities	11
5. Secure framework for RIC	12
5.1 Security aspects of near-real-time radio intelligent controller (Near-RT RIC)	12
5.1.1 Secure Interface between Near-RT RIC and the O-CU-CP / O-CU-UP / O-DU	12
5.1.2 Conflict resolution and xApp authentication	12
5.1.3 User identification inside the Near-RT RIC	13
5.2 Security aspects of Non-Real-Time Radio Intelligent Controller (Non-RT RIC)	13
5.2.1 Secure Interface between Non-RT RIC and the O-CU-CP / O-CU-UP / O-DU	14
5.2.3 Conflict resolution between the Non-RT RIC and the O-CU-CP / O-CU-UP / O-DU	14
6. Secure platform for Network Elements	15
6.1 Secure platform for cloud native network functions	15
6.1.1 Security of a container-based application software	16
6.1.2 Security of cloud native software infrastructure	18
6.1.3 Security considerations with a cloud native hardware infrastructure	21
6.2 Secure platform for O-RU	22
7. Key security differentiators in Open RAN	23
8. Conclusion	24
Appendix	25
References	25
Acronyms	25

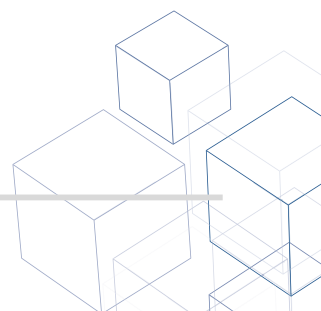


Table of Figures

Figure 1: gNB Logical Architecture in 3GPP	5
Figure 2: gNB Logical Architecture in O-RAN	5
Figure 3: Interfaces and Functions split between O-RAN and 3GPP	6
Figure 4: 5G RAN Network Security Architecture	8
Figure 5: Certificate-based device authentication of O-CU, O-DU and O-RU	10
Figure 6: Non-Real-Time RIC declarative policies and objective intents	13
Figure 7: Cloud native platform	15
Figure 8: Security built into all phases of a software development process	16
Figure 9: Automated security practices based on DevSecOps	17
Figure 10: Secure boot using a hardware root of trust.....	21

Definitions

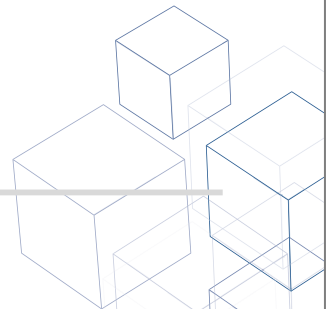
Network Service (NS): A composition of network functions defined by its functional and behavioral specification. In the RAN Context, a gNB is a Network Service.

Network Function (NF): A functional building block within a Network Service, with well-defined interfaces and behavior. In the O-RAN Alliance's RAN architecture context, a O-DU, O-CU-CP, O-CU-UP, Near-RT RIC and Non-RT RIC are Network Functions.

Cloud Native Network Function (CNF): CNF is one type of manifestation of a NF (like VNF or PNF) deployed as a decomposed set of containerized

microservices. In a cloud native realization of O-RAN Alliance's RAN architecture, the managed entities, O-CU-CP, O-CU-UP, O-DU, Near-RT RIC, Non-RT RIC and Service Management and Orchestration (SMO) are CNFs. CNF and NF are interchangeable in the context of 5G cloud native services.

Physical Network Function (PNF): This refers to network functions that are not virtualized. In the O-RAN Alliance's RAN architecture context, the O-RUs that are deployed at a cell site can be considered PNFs.



1. Overview

Open RAN is an open radio access network (RAN) architecture standardized by the O-RAN Alliance based on 3GPP and other standards. O-RAN Alliance's RAN functional split is based on the three key tenets:

- Decoupling of hardware and software
- Cloud infrastructure
- Standardized and open interfaces between the network functions

In the IT world, hardware-software decoupling happened a long time ago. This decoupling led to the emergence of software players that were experts in specific horizontal layers. The software from these players could run on any hardware providing operator customers with a variety of options. An equally rich ecosystem of hardware players emerged.

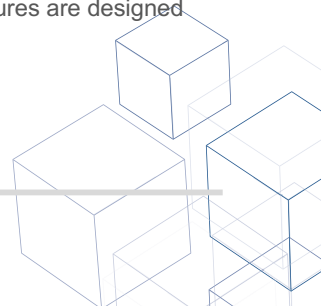
Virtualization technologies have helped enterprises reduce their TCO through efficient use of compute resources, removal of hardware silos and increased automation. To deliver 5G services, operators need a virtualized network capable of scaling services based on policy-driven service selections for subscribers. Cloud native architecture allows deployment of network functions (NFs) as a cluster of containerized microservices, where each microservice can be deployed, scaled, and upgraded independently. Instead of scaling the whole application, only the required component within the NF is scaled.

Open interfaces between various network functions allow best of breed equipment to be used in networks enabling operators to distinguish themselves from competition by using bespoke network functions, as needed.

In this paper it is demonstrated how, by adopting a zero-trust security framework, an Open RAN architecture provides a path to a more secure open networks and open interfaces over what exists today. Despite misconceptions, open interfaces, defined in the O-RAN technical specifications, provide increased independent visibility and the opportunity for an overall enhanced and more secure system.

5G and Open RAN enable new capabilities and control points that allow suppliers, test equipment manufacturers, wireless carriers, and network operators to assess, mitigate and manage security risks efficiently. This paper details how O-RAN enables operators with full visibility and control of their network's end-to-end security.

There is a vast cloud industry solving security issues, and cloud RAN network functions are similar to other cloud network functions, with similar security requirements and solutions. Cloud architecture ensures resilience, scalability and segmentation and the introduction of features such as AI/ML and Multi-Access Edge Computing (MEC). For example, leveraging MEC, allows collection and processing of sensor traffic at a factory to shift DDoS detection and mitigation to the edge of the network where incidents at the edge can be isolated from the rest of the network. Microsegmentation, containerization, virtualization, and network slicing provide enhanced security and isolation from the hardware up. The security measures are designed into the system rather than being bolted on afterwards as in traditional systems.



2. Next Generation RAN Architectures

3GPP [1] has defined the following architecture for 5G NR gNB as shown in **Figure 1**.

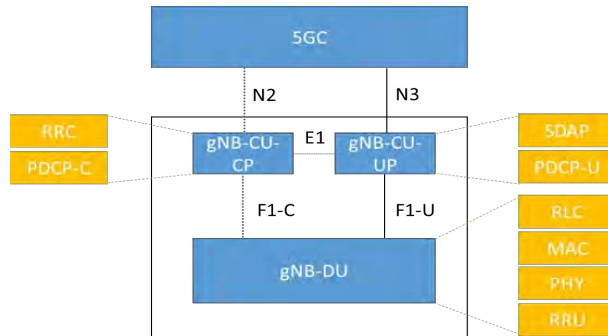


Figure 1: gNB Logical Architecture in 3GPP

gNB is split into two logical functions called CU (Centralized Unit) and DU (Distributed Unit) as shown in **Figure 1** and these two entities are connected by F1-C and F1-U interfaces as defined in 3GPP TS 38.473[2]. It may be noted that the 3GPP architecture does not specify the Remote Radio Unit (RRU) i.e. the interface between PHY and RF layers is left to vendor implementation.

O-RAN Alliance, a group of leading vendors and operators defining Open RAN specifications, further disaggregate CU and DU network functions [3] as defined by 3GPP that are inter-connected over open, standardized, secure interfaces as shown in **Figure 2**.

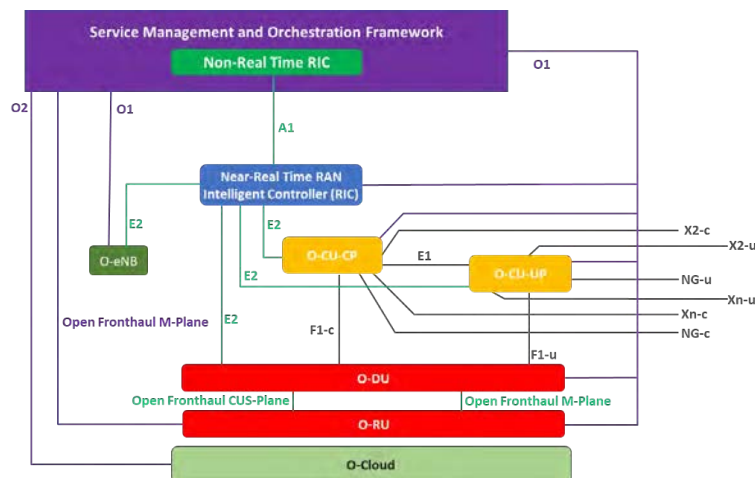


Figure 2: gNB Logical Architecture in O-RAN

Figure 3 shows the functional and interface split between 3GPP and O-RAN. The O-RAN Alliance adds new interfaces and functions beyond 3GPP's 5G RAN architecture.

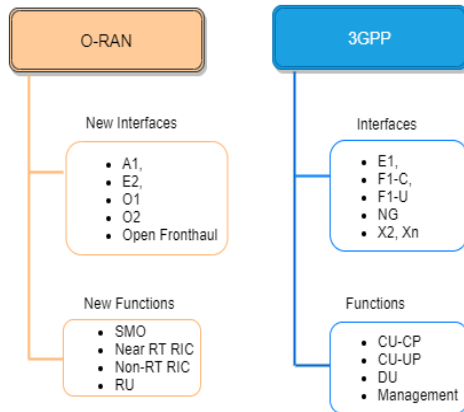
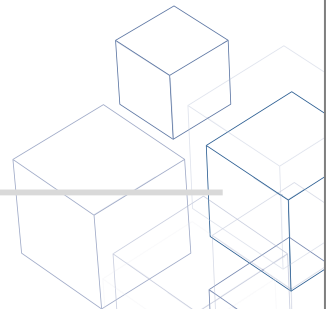


Figure 3: Interfaces and Functions split between O-RAN and 3GPP

Since O-RAN Alliance builds on 3GPP's 5G NR architecture, it benefits from 3GPP's advanced security features introduced for 5G [4] including:

- Enhanced user identity privacy i.e., Subscription Concealed Identifier (SUCI)
- Full protection of control/user plane traffic between the UE and gNB (encryption and integrity protection) over the air interface
- Full protection of gNB interfaces including the E1 interface between CU-CP and CU-UP and the F1 interface between CU and DU
- Enhanced home network control (authentication)
- Additional security for network slices based on SLA



3. Open RAN security based on Zero Trust Architecture

Rooted in the principle of “never trust, always verify,” Zero Trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control.

A zero trust architecture (ZTA) is a cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement. The following is the relevant text from NIST publication 800-207 - ‘Zero Trust Architecture’ [5]-

A “zero trust” (ZT) approach to cybersecurity is primarily focused on data and service protection but can and should be expanded to include all enterprise assets (devices, infrastructure components, applications, virtual and cloud components) and subjects (end users, applications and other nonhuman entities that request information from resources).

In this new paradigm, an enterprise must assume no implicit trust and continually analyze and evaluate the risks to its assets and business functions and then enact protections to mitigate these risks. In zero trust, these protections usually involve minimizing access to resources (such as data and compute resources and applications/services) to only those subjects and assets identified as needing access as well as continually authenticating and authorizing the identity and security posture of each access request.

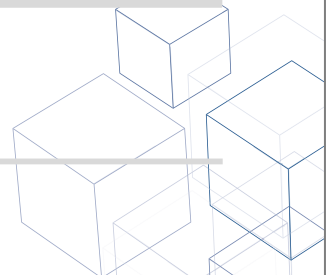
Support of a zero-trust architecture requires each O-RAN component to comply with established functionalities and protections. O-RAN Alliance [6] has identified several guiding principles for its ongoing work, including:

1. Support integration with an external identity, credential and access management system (ICAM) using industry standard protocols
2. Require authentication and authorization on all access
3. Support role-based access control (RBAC)
4. Implement confidentiality on connections between O-RAN and external components
5. Implement integrity checking on connections between O-RAN and external components
6. Support encryption of data at rest
7. Support replay prevention
8. Implement security log generation and collection to an external security information and event management (SIEM)

Open RAN security is built on the following tenets:

1. Secured communication between Network Functions
2. Secure framework for the Radio Intelligent Controller (RIC)
3. Secured platform for hosting the Network Functions

The analysis in the following sections assumes a cloud native Open RAN network with Network Functions modeled as containerized microservices.



4. Secured communication between Network Functions

This section explores following areas that relate to providing secure communication between all Network Functions in Open RAN.

- Secure communication on all interfaces
- Ensuring trust based authentication of communicating endpoints
- Trusted Certificate Authorities for Identity Provisioning

4.1 Secure communication on all interfaces

O-RAN Alliance specifies an open and secure architecture that includes secure interfaces between all its components. Communications exchanged on these interfaces are cryptographically protected for encryption, integrity protection and replay protection.

Figure 4 depicts the 5G RAN network security architecture.

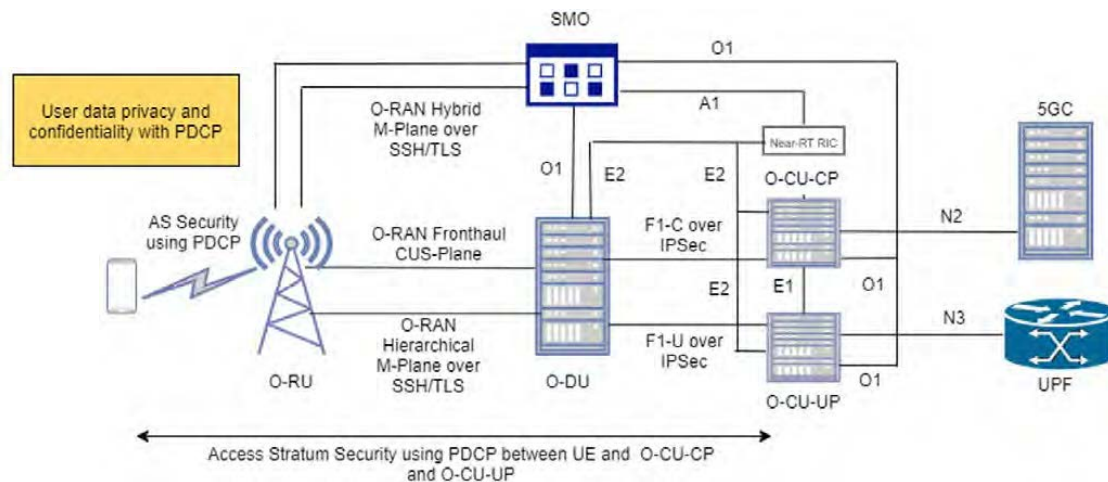


Figure 4: 5G RAN Network Security Architecture

The following table summarizes the protection mechanism used for each interface in an O-RAN based network.

Interface	Between nodes	Security mechanism	Specified by
E1	O-CU-CP and O-CU-UP	NDS/IP (IPSec) or DTLS	3GPP
Xn	Source gNB and Target gNB	NDS/IP (IPSec) or DTLS	3GPP
Backhaul	O-CU-CP and 5GC (N2) O-CU-UP and 5GC (N3)	NDS/IP (IPSec) or DTLS	3GPP
Midhaul (F1)	O-CU-CP and O-DU (F1-C) O-CU-UP and O-DU (F1-U)	NDS/IP (IPSec) or DTLS	3GPP
Open Fronthaul (M-Plane)	O-RU and O-DU/SMO	SSHv2, TLS	O-RAN WG4
Open Fronthaul (CUS-Plane)	O-DU and O-RU	Work in progress (Dec 2020)	O-RAN WG1 STG
O1	SMO and O-RAN Managed elements	Work in progress (Dec 2020)	O-RAN WG1 STG
E2	Near-RT RIC (xAPPs) and O-CU-CP	Work planned (1Q21)	O-RAN WG1 STG
A1	Near-RT RIC and Non-RT RIC	Work planned (1Q21)	O-RAN WG1 STG
O2	SMO and O-Cloud	Work planned (2Q21)	O-RAN WG1 STG

It should be noted that several O-RAN Alliance specifications are still on-going and accordingly security work is happening in parallel. For protection of the CUS-Plane messages [7] on Open Fronthaul LLS interface, O-RAN Alliance is currently in the process of determining all the threats and vulnerabilities, and their impact on the CUS-Plane. O-RAN Alliance plans to complete the analysis and specify security procedures to protect CUS-Plane messages by March 2021.

4.2 Establishing trust based on mutual authentication

Mutual authentication is used for authenticating two entities with each other and setting up a secure encrypted connection between them. Mutual authentication prevents introduction of rogue NFs or xAPPs in the network.

Operator X.509 certificates are used for mutual authentication while establishing secure connections using IPsec and TLS protocols.

All network elements in an Open RAN, i.e. O-CU-CP, O-CU-UP O-DU and O-RU, support X.509 certificate-based authentication and related features such as auto-enrollment and auto-re-enrollment with an operator Certificate Authority (CA) server using a protocol such Enrollment over Secure Transport (EST) or 3GPP-specified CMPv2.



The xAPPs in the Near-RT RIC are securely on-boarded like any other microservice and the O-RAN Alliance is expected to use CA signed X.509 certificates to authenticate before communicating over the E2 interface.

Figure 5 illustrates an example flow of how certificate-based authentication is used to authenticate an O-CU, O-DU and O-RU during certificate enrollment with a CA server.

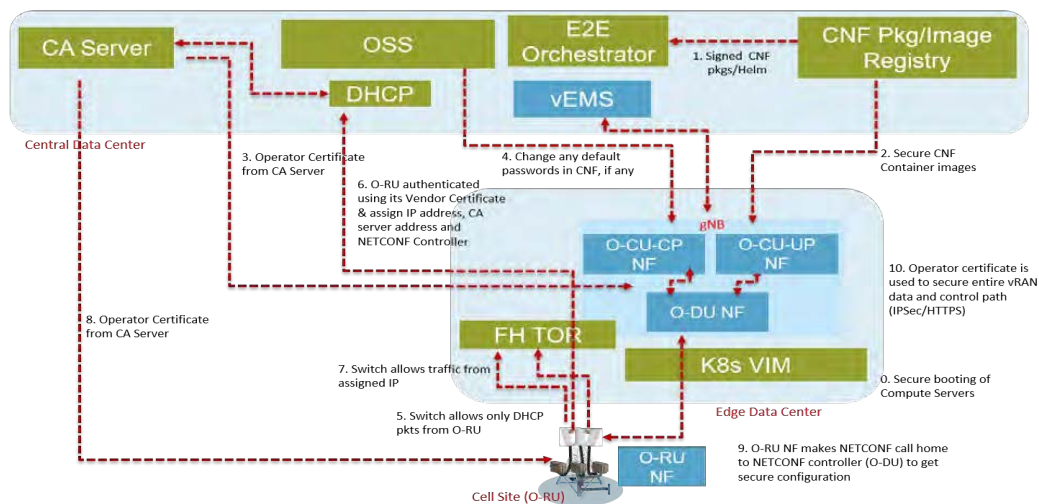


Figure 5: Certificate-based device authentication of O-CU, O-DU and O-RU

Step 1-2: When the O-RU powers on, the O-CU-CP, O-CU-UP and O-DU instances that are allocated to serve that O-RU are instantiated by the orchestrator, if not already instantiated.

Step 3: an O-CU-CP, O-CU-UP and O-DU performs EST or a CMPv2-based certificate enrollment procedure in compliance with 3GPP with the CA server to obtain an operator certificate. The operator certificate is used for subsequent authentication when establishing an IPSec or a TLS connection.

Step 4: necessary OAM actions are performed on the O-CU, if any, including changing of default passwords.

Steps 5 thru 9 are executed as part of the O-RU power-on sequence. Key security related steps are explained below:

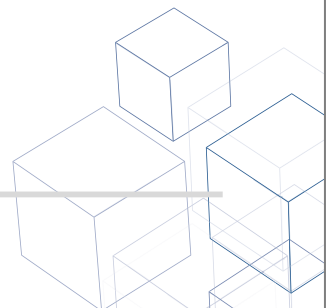
- The O-RU obtains its IP address, the EMS or OSS address from a DHCP server using one of the DHCP options specified in O-RAN M-Plane specification section 3.1.1 and 3.1.4 [8].
- The O-RU performs certificate enrollment procedure with the CA server to obtain an operator certificate. The vendor-provisioned device certificate is used for authenticating with the CA server.

- *The O-RU shall notify the EMS or OSS with a NETCONF call home. O-RU's operator certificate is used to authenticate with the EMS. OSS / EMS shall configure the O-RU with the secondary NETCONF controller's address (i.e. the address of the O-DU).*
- *The O-RU shall notify the O-DU with a NETCONF call home to securely obtain O-RU's configuration. O-RU's operator certificate is used to authenticate with the O-DU.*

4.3 Trusted Certificate Authorities

It is recommended that the certificate authorities (CA) should be audited under the AICPA/CICA WebTrust Program for Certification Authorities.

This promotes confidence and trust in the CA servers used in Open RAN for authenticating network elements.



5. Secure framework for RIC

5.1 Security aspects of near-real-time radio intelligent controller (Near-RT RIC)

The Near-RT RIC is an SDN component that contains 3rd party extensible microservices (called xApps) that perform selected radio resource management (RRM) services for the NFs that were traditionally managed inside the gNB. The Near-RT RIC interfaces with the O-CU-CP, O-CU-UP and the O-DU via the O-RAN standardized open E2 interface. The Near-RT RIC also interfaces with the Non-RT RIC and the service management and orchestration framework via the A1 and O1 interfaces.

The key security aspects of the Near-RT RIC include:

- Secure E2 Interface between the Near-RT RIC and the O-CU-CP / O-CU-UP / O-DU
- Conflict resolution and xApp authentication
- User identification inside the Near-RT RIC

5.1.1 Secure Interface between Near-RT RIC and the O-CU-CP / O-CU-UP / O-DU

Interface security is explained in § 4.2

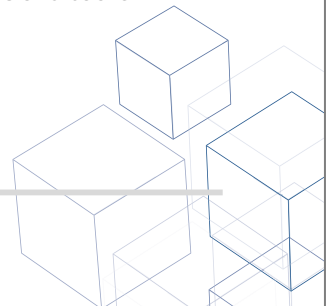
5.1.2 Conflict resolution and xApp authentication

The conflict resolution among the xApps is not necessarily a security issue but can lead to vulnerabilities if not handled properly.

While the xApps in the Near-RT RIC initiate the RIC subscription procedure with the E2 nodes, the subscription manager in the Near-RT RIC platform, enforces the subscription policies and keeps track of the subscriptions initiated by the xApps and the RAN functions, and event triggers associated with those subscriptions. The subscription manager can resolve signaling conflicts among the xApps by one or more of the following means:

- The subscription manager will not allow more than one xApp to subscribe to the same NF based on the same event trigger.
- If more than one xApp subscribes to the same NF and gets the same indication messages from the E2 node, then the subscription manager can allow them to simultaneously control the NF of the E2 node, as long as they do not optimize the same or closely inter-dependent parameters pertaining to the NF.
- If more than one xApp subscribes to the same NF and gets the same indication messages from the E2 node and if they optimize closely inter-dependent parameters, then the subscription manager can allow them to simultaneously control and optimize those parameters by using locks and backoff timers to retain mutual exclusivity.

Authentication aspects of xAPP is explained in § 4.2



5.1.3 User identification inside the Near-RT RIC

Maintaining privacy of the users is of utmost importance inside the RIC. ORAN WG3 is working on the UE identification inside the Near-RT RIC that can be addressed by a combination of 3GPP-defined Trace ID, 3GPP-defined RAN UE ID, temporary RAN network interface-specific UE IDs, and by correlating these IEs with one another. Typically, it is ideal for the Near-RT RIC to maintain persistence of UE identification for near-RT granularities, ranging from 10 ms to 1 s. The xApps are not exposed to UE permanent ID. Invalidation of the temporary IDs in the RIC when they are released in RAN nodes will be handled via normal E2 communication. In neither case is this a UE privacy issue or a DoS attack threat.

5.2 Security aspects of Non-Real-Time Radio Intelligent Controller (Non-RT RIC)

The Non-RT RIC is a component in an O-RAN system for non-real-time control of the RAN through declarative policies and objective intents. This is illustrated in **Figure 6** below.

1. The Non-RT RIC is deployed in a service management and orchestration framework (SMO) and provides declarative policy guidance for cell-level optimization by providing the optimal configuration values for cell parameters over the O1 interface.
2. The Non-RT RIC also sends declarative policies for UE-level optimization to the Near-RT RIC via the A1 interface.
3. The Near-RT RIC then translates the recommended declarative policy from the Non-RT RIC over A1 interface into per-UE control and imperative policy over the E2 interface.
4. The Non-RT RIC develops ML/AI-driven models for policy guidance and non-RT optimization as rApp microservices. These rApps interface with the xApps over the A1 interface to optimize a set of procedures and functions in the underlying RAN.

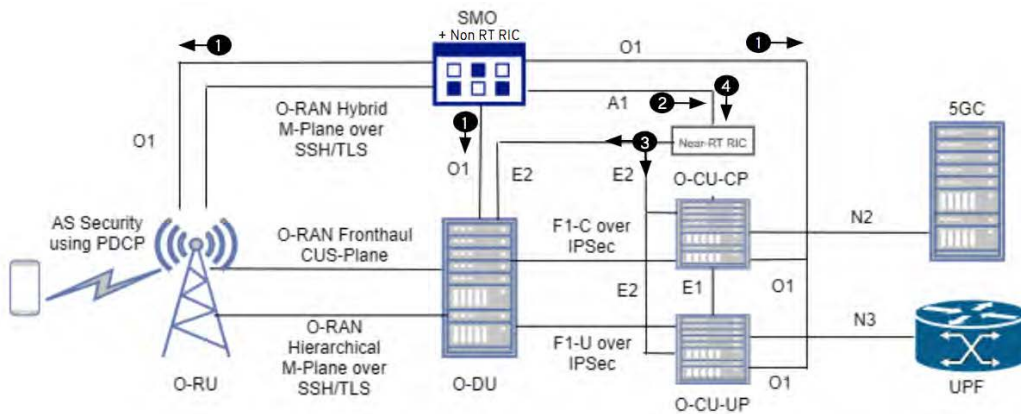


Figure 6: Non-Real-Time RIC declarative policies and objective intents

The key security aspects of the Non-RT RIC are the following:

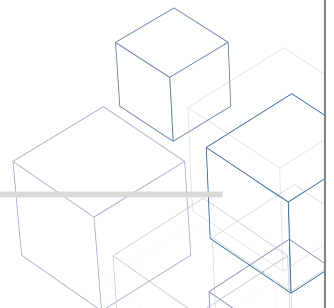
- Secure interface between Non-RT RIC and the O-CU-CP / O-CU-UP / O-DU
- Conflict resolution between the Non-RT RIC and the O-CU-CP / O-CU-UP / O-DU

5.2.1 Secure Interface between Non-RT RIC and the O-CU-CP / O-CU-UP / O-DU

Interface security is explained in § 4.2

5.2.3 Conflict resolution between the Non-RT RIC and the O-CU-CP / O-CU-UP / O-DU

Usually, a conflict in RRM arises when the RAN uses policies and objective intents different from the Non-RT RIC to manage the underlying RAN nodes such as the O-CU. This may be the source of rApps causing signaling conflicts with the functioning of the underlying RAN nodes. However, using the RIC subscription policies, mutual exclusivity can be enforced causing the subscribed procedures from the RAN to be managed by the Near-RT RIC, without causing signaling conflicts.



6. Secure platform for Network Elements

O-RAN Alliance RAN architecture is built on a fully cloud native architecture – the same cloud architecture that is the bedrock of today's internet and public cloud. The cloud native network functions in the O-RAN network viz. O-CU-CP, O-CU-UP, O-DU, Near-RT RIC and Non-RT RIC, are hosted on a cloud native platform, very similar to the cloud native platform used in the cloud computing industry. The O-RU is a PNF and thus hosted on a non-virtualized platform.

In the following sections we take a holistic look at security aspects of these platforms.

6.1 Secure platform for cloud native network functions

The O-RAN architecture uses a cloud-native platform to host O-CU-CP, O-CU-UP, O-DU, Near-RT RIC and Non-RT RIC network functions. **Figure 6** shows a typical cloud native platform with three distinct layers:

1. Container-based application software
2. Cloud native software stack comprising an immutable OS, Kubernetes and Container runtime
3. Cloud native hardware infrastructure

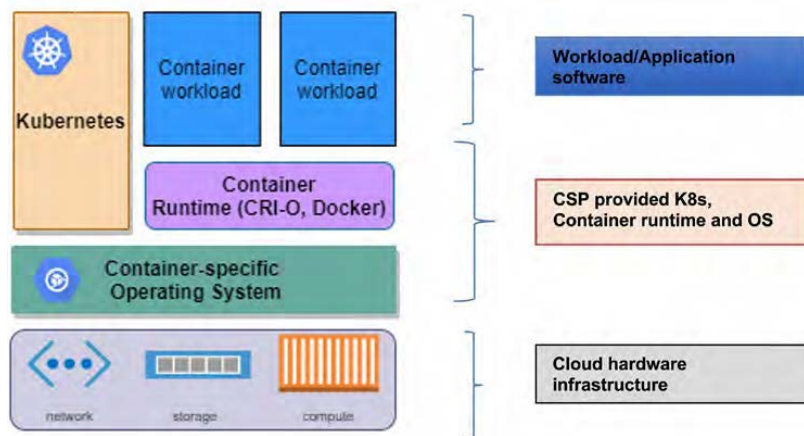
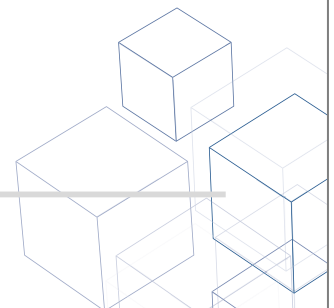


Figure 7: Cloud native platform

The following sections look at security features of each of the three layers that make up a cloud native platform.



6.1.1 Security of a container-based application software

A workload is an application or a service deployed on the cloud. Containers offer a packaging infrastructure in which applications and dependent libraries are abstracted from the environment in which they actually run.

Containers are generally perceived to offer less security than virtual machines. But it's worth noting that containers have been in use in the IT industry to build applications such as for banking which are no less critical than telecom applications in terms of security requirements, and the industry has evolved itself in automating its security and establishing best practices.

The following industry standard practices are used in Open RAN to ensure security of the container-based application software:

- a) Secure software development based on “secure by design” principles
- b) Automating security testing based on DevSecOps
- c) Vulnerability management in Open Source and 3rd party libraries

Secure software development based on “secure by design” principles

A software development life cycle (SDLC) is a framework for the process of building an application from inception to decommission. In the past, organizations usually performed security-related activities only as part of testing—at the end of the SDLC. As a result of this late-in-the-game technique, they wouldn't find bugs, flaws, and other vulnerabilities until they were far more expensive and time-consuming to fix. Worse yet, they wouldn't find any security vulnerabilities at all.

A secure SDLC involves integrating security testing and other security-related activities into an existing development process. **Figure 7** shows how a standard SDLC process is augmented with security practices at every stage of software development.

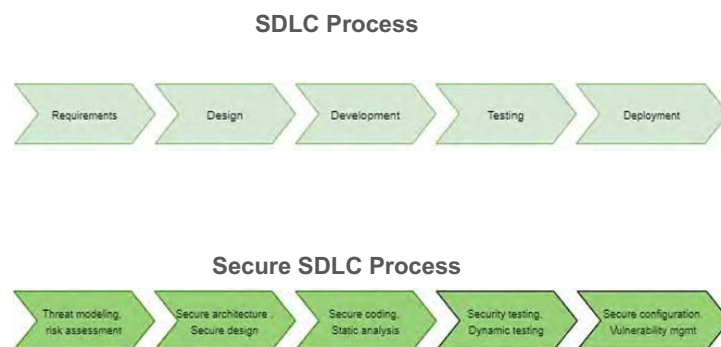


Figure 8: Security built into all phases of a software development process

Using a secure SDLC process for the workloads deployed in a O-RAN network such as xAPPs in Near-RT RIC, O-CU-CP and O-CU-UP and O-DU microservices, ensures early detection of flaws in the system, awareness of security considerations by all stakeholders involved in designing, development, testing and deployment of containers, and overall reduction of intrinsic business risks for the organization.

Automating security testing based on DevSecOps

Since the beginning of modern computing, security testing has largely been an independent activity from software development. Security focused QA professionals performed testing during the testing phase.

A DevSecOps approach to the container development lifecycle ensures that security is built-in at every stage of the CI/CD pipeline.

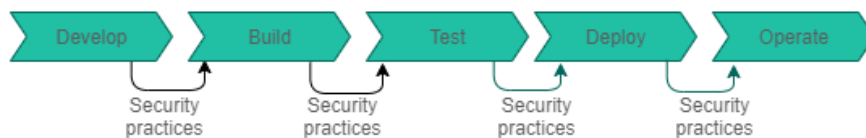


Figure 9: Automated security practices based on DevSecOps

The philosophy behind DevSecOps is to begin security testing early in the SDLC. DevSecOps integrates various security controls into the DevOps workflow such as secure coding analysis using static application security testing (SAST), automated unit, functional and integration testing. This enables developers to fix security issues in their code in near real time rather than waiting until the end of the SDLC.

O-RAN Alliance architecture software takes advantage of the advancements in 'security automation' and trend in cloud computing towards "shift left." This ensures that workloads run in the O-RAN network are validated securely (during build/deployment phase) and risk-based timely actions are taken when vulnerabilities are found before they are deployed in operator network.

Vulnerability management of open source and 3rd party libraries

Open source libraries and open source software enable developers to meet the demands of today's accelerated development timelines. However, they can also open up the platform to attacks due to unaddressed vulnerabilities in the software.

Software component analysis (SCA) is an open source management tool that helps in identifying potential areas of risk from the use of third-party and open-source software. SCA software automatically scans all open-source components, creates an accurate bill of materials (BOM), checks for policy and license compliance, security risks, and version updates. SCA software also provides insights for remedying identified vulnerabilities, usually within the reports generated after a scan.

Specialized container image scanning tools provide automated vulnerability management for containers by identifying and providing remediation paths for all the vulnerabilities in the image. These tools are integrated into the CI/CD pipeline and provide continuous assessment of the container image.

Use of software component analysis tools in an O-RAN network allows for deployment of an advanced vulnerability management process that includes automatic tracking, analysis of an application's open source components, identification of component vulnerabilities, and tool-based vulnerability remediation.

Compliance with supply chain risk management requirements from NIST SCRM and CISA ICT SCRM.

6.1.2 Security of cloud native software infrastructure

A cloud native software infrastructure includes the following:

- a. Container-specific operating system – lightweight and purpose-built OS
- b. Container runtime – software that executes containers and manages container images on a node
- c. Container orchestration – software that automates the deployment, management, scaling and networking of containers

Container-specific OS

The cloud native software infrastructure relies, in line with the NIST SP 800-190 recommendations [9], on a host OS built and configured for the sole purpose of running containerized applications instead of general-purpose applications reducing the OS attack surface. In addition, the container-specific OS follows the immutability infrastructure paradigm by preventing any additional individual software package installation protecting against viruses and malware; the entire OS being managed as a single entity. Any additional feature has to be installed as a container. The OS implements strong isolation and mandatory access control (MAC) mechanisms such as SELinux to limit what a container can do and thus protecting the OS from the containers and the containers from each other. The OS also supports inbuilt Linux features such as control groups (cgroups) and namespaces that provide an isolated environment for the application running inside the container. The OS also supports disk encryption including the root partition by leveraging linux unified key setup (LUKS) encryption.

Container runtime

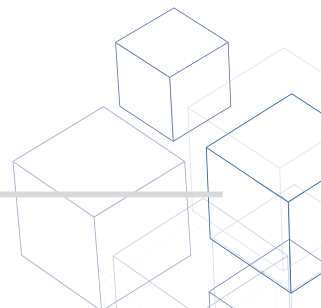
The cloud native software infrastructure includes a lightweight, Kubernetes-specific OCI-compliant container runtime versioned with Kubernetes such as CRI-O to reduce the risk of vulnerabilities.

The cloud native software infrastructure (container -specific OS, container runtime, disk ...) must support running in FIPS mode by using FIPS 140-2 validated cryptography.

Native security with Kubernetes

Kubernetes provides several built-in security capabilities to secure the container environment including network security, resource isolation, access control, logging and auditing. Some of the common Kubernetes built-in controls that help in tightening security include:

- a) Role based access control (RBAC)



Use of RBAC in the cluster provides a framework for implementing the principle of least privilege for humans and applications accessing the Kubernetes API.

b) Configure the security context for pods to limit their capabilities

Pod security policy sets defaults for how workloads are allowed to run in the cluster. These controls can eliminate entire classes of attacks that depend on privileged access.

c) Use Kubernetes network policies to control traffic between pods and clusters.

Kubernetes' network policies allow control of network access into and out of the containerized applications. In addition to this feature, software-based firewalls may be deployed to control container to container communication within or across different clusters.

d) Use namespaces to isolate sensitive workloads and create security boundaries – separating workloads into namespaces can help contain attacks and limit the impact of mistakes or destructive actions by authorized users.

e) Assess the container privileges – Adhering to the principle of least privilege and provide the minimum privileges and capabilities that would allow the container to perform its intended function.

f) Use mutual Transport Layer Security (TLS) for all inter cluster and intra cluster communications.

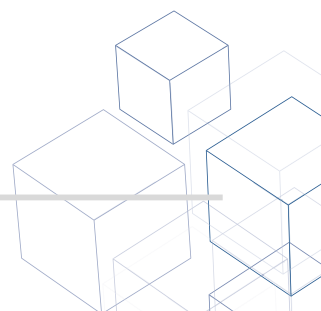
g) Capability to encrypt the etcd datastore to protect infrastructure and application secrets or to support integration with external vaults.

Leveraging Kubernetes operators for security

Kubernetes operators are software extensions to Kubernetes that make use of custom resources to manage services and their components in an automated way. These operators can be leveraged by the cloud native software platform for specific security purposes:

- Hardware management operators to restrict the need for applications of elevated privileges
- Compliance operators to continuously monitor the compliance of the cluster
- File integrity monitoring operators to detect any attacks impacting the platform integrity
- Platform management operators to fight configuration drift and enforce a secure configuration by eliminating human errors
- Audit and log operators to manage the audit configuration and the log forwarding to a SIEM

A cloud native-based O-RAN network can leverage native security controls in container runtime and container orchestration platforms such as Kubernetes, to provide defense in depth security for the containerized workload that they host.



Secure configuration of the cloud infrastructure based on industry benchmarks

The cloud infrastructure is configured based on industry best practices such as CIS benchmarks for operating system, Docker and Kubernetes, and Network Equipment Security Assurance Scheme (NESAS) jointly defined by 3GPP and GSMA provides a consistent framework and common external audit program for multiple vendors and operators. This ensures that appropriate security controls are put-in-place in the platform, thus reducing its attack surface.

Some of the common security controls include disabling unused ports and unused service, principle of least privileges (PLoP) for workloads, protecting data in storage, user access control using RBAC, etc.

All virtualized platforms in an O-RAN network are hardened as per 3GPP's security assurance specifications [10] and other well-known industry benchmarks such as those from CIS [11]. This ensures that security controls are implemented at every layer of the platform thus reducing the platform's attack surface.

Detecting and remediating configuration errors with cloud security posture management

Misconfiguration is the #1 cause of cloud-based data breaches. A mechanism is needed to make sure the configuration of the deployed cloud resources is correct and secure on day one, and that they stay that way on day two and beyond. This is referred to as cloud security posture management (CSPM).

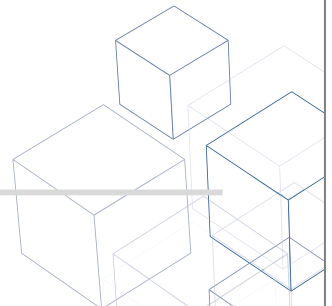
The cloud industry has used CSPM security tools to continuously monitor cloud environments for detection of cloud misconfiguration vulnerabilities that can lead to compliance violations and data breaches.

With the adoption of a cloud native architecture in O-RAN based networks, an operator now has the means to deploy advanced CSPM tools to guard against natural "drift" of on network configuration and reduce the potential for attacks.

Commercial cloud native hybrid platform

Standardizing on a commercial cloud native hybrid platform enables the operator with the following security benefits:

- A Kubernetes-certified platform with the flexibility to run securely on-prem or in a virtual private cloud, supporting O-RAN topology variations from the SMO, RICs, CUs, and DUs with zero-touch provisioning,
- Extended software lifecycle with dynamic updates that address new CVEs and optimizations over time into disconnected environments,
- Support for multi-tenancy so that multi-vendor software can be securely hosted in the same cluster,
- Support for infrastructure compliance scanning (OpenSCAP) and remediation,
- A container registry with vulnerability scanning to eliminate vulnerabilities on O-RAN platforms (e.g Near Real-Time RIC) and associated xApps and rApps.



6.1.3 Security considerations with a cloud native hardware infrastructure

O-RAN enables decoupling of hardware and software, allowing for a platform to be built from different vendors.

6.1.3.1 Secure storage of credentials and data at rest

It is recommended that O-RAN hardware comes with a hardware-based security module like TPM to manage, generate, and securely store cryptographic keys. Hardware-based security modules are also meant to provide a hardware root of trust to enable secure computing by providing a secure key storage enclave with minimal cryptographic functions primarily in the signing and signature verification space.

The data at rest must be encrypted using keys generated from hardware-based security modules.

6.1.3.2 Establishing software chain of trust

Zero-trust cannot be achieved without the full participation of all the elements in the trust chain for a network. **Figure 9** illustrates key aspects of establishing chain of trust when adhering to zero-trust in digital systems.

Trusted hardware

The hardware is built with a tamper resistant “hardware root of trust” device that provides a secure environment for storing cryptographic keys and for attestation of certificates and all the software running on that hardware. The device will expose a simple user interface for the application to use when it needs to use the device for storing keys, retrieving certificates etc.

Trusted software

Software signing is enforced at all software layers including the firmware, cloud native software stack and container workloads at time of deployment, as well as authenticated version upgrades to make it more difficult to introduce malicious software into operator-controlled elements.

Establishing end-to-end chain of trust with secure boot

Secure boot requires that every boot up is starting from a piece of software that cannot be updated in the field. This piece of software is referred to as Core Root of Trust for Measurement (CRTM).

Thereafter, during the boot process every software program in the platform will be integrity verified before its execution by the software at the lower layer. This establishes an end-to-end software chain of trust. The trust anchor for the software integrity verification is software signing certificate.

In the O-RAN network, it is recommended to use secure boot based on hardware root of trust and software signing to establish an end-to-end chain of trust.

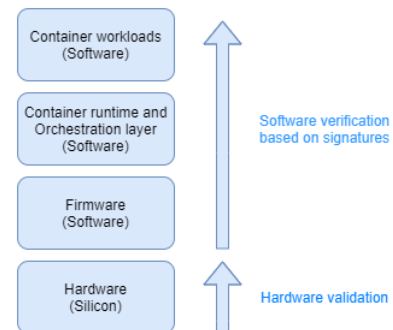
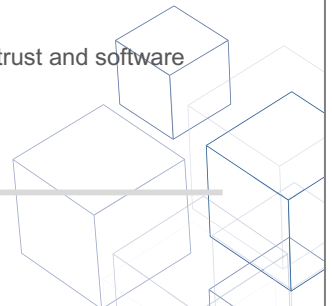


Figure 10 Secure boot using a hardware root of trust



6.2 Secure platform for O-RU

An attacker with unauthorized access to the management interface of an unprotected O-RU could allow an attacker to steal unprotected private keys, certificates, hash values and/or inject malwares and/or manipulate existing O-RU software. An attacker could further launch denial-of-service, intrusion, and replay attacks on other network elements including an O-DU.

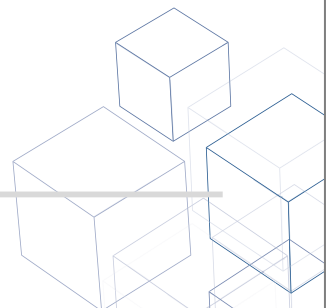
Therefore, hardening of the O-RU platform will ensure enough equipment security to substantially reduce the attack surface that would otherwise exist in an unprotected O-RU. Security precautions on the O-RU can be divided into three aspects.

1. Supply chain security
2. Physical security
3. Network security

Supply chain security ensures that throughout the supply chain process of manufacturing, from O-RU to its final installation site and commissioning, a controlled secure chain of custody process is followed. This ensures that the O-RU is properly tracked and tagged.

Physical security ensures that the physical O-RU is sealed with non-tamper-able screws that cannot be easily broken or opened and in the event of tampering or forced opening, all O-RU functionality will be disabled so that the O-RU becomes inoperable. This is in addition to all the physical and logical ports being secured and isolated, so that they cannot be used as a vulnerability entrance into the extended RAN network.

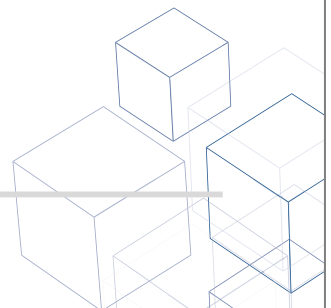
From a network security point of view, O-RU ensures that all authentication and communication security protocols are correctly performed and followed. To ensure reliable and secure software upgrades, the TPM procedures are implemented so that rogue software downloads are prevented. Finally, hardening features, such as disabling unnecessary software components and interfaces when not in use, running software at the correct privilege-level, scrambling/encryption of data in storage, and secure boot and hardware-based security module, are part of the comprehensive security processes on the typical O-RU to ward off as well as prevent unauthorized access to the O-RU.



7. Key security differentiators in Open RAN

The following table highlights some of the key differentiators that Open RAN provides compared to a closed RAN or the classical gNB.

Differentiator	Open RAN	Closed RAN
Security of open fronthaul	Provides visibility to the security measure taken to protect this interface. Open, standardized interfaces remove vulnerabilities or risk that comes with proprietary and potentially untrusted implementation.	Protection measure taken to protect CPRI interface in a closed RAN is not known
Operator has full control in building a secure platform	Open RAN's disaggregated architecture allows network operators to build cloud-native platforms by selecting suppliers that meet all the required industry security standards and certifications.	Operator has no control of how the virtualized platform is assembled. It is fully vendor driven.
Better enforcement of security controls in cloud infrastructure	A cloud infrastructure supplier will be directly under an agreement with the operator and will be responsible for security of the cloud infrastructure.	Operator has no direct visibility of the cloud infrastructure provider
Disaggregated platform allows for better visibility and automated monitoring of the network	A cloud native architecture allows operators to deploy the latest security tools for monitoring vulnerabilities and automated remediation measures as required	Operator has no visibility to this information. The operator is fully dependent on the vendor to detect and remediate vulnerabilities in the network
Adoption of industry best practices in development of containerized applications	Allows adoption of industry best practices such as "secure by design" DevSecOps, automated testing in development of containerized applications. Operator also has an option to work with the supplier to determine and influence CI/CD processes used by the supplier.	It is fully vendor driven, and an operator has no mechanism to verify the software development process used by the vendor.
Protection of cryptographic key	NG-RAN cryptographic key (KgNB) is stored in CU, which is located in a centralized data center inside the network.	Stored at the cell site and can be potentially stolen especially when HSM is not implemented in gNBs.



8. Conclusion

At the heart of Open RAN is the use of cloud native architecture, the same architecture that is the bedrock of today's internet and public cloud. Security practices in virtualized deployments are mature and used across the cloud computing industry. Virtualized deployment in telecom networks is not new. Operators already have virtualized infrastructure in their data centers and many have deployed virtual workloads for other components in the network including: packet core, IMS, and other applications such as CDN. With a disaggregated architecture, operators will now additionally benefit from security expertise and experience of today's large cloud infrastructure suppliers in managing the security of large IT cloud environments.

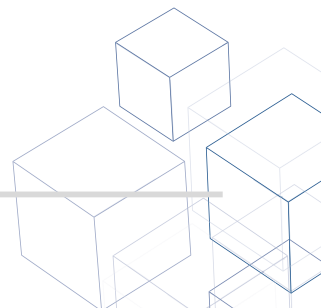
Operator regains control as the operator now understands what is required to build and maintain a secure infrastructure. Open RAN is built on a cloud native platform with clear responsibilities and accountability established between hardware/infrastructure suppliers, a hybrid-cloud platform supplier, and RAN software suppliers. It enables network operators to select suppliers that meet all the required industry security standards and certifications.

Open RAN leverages several security industry best practices used in the cloud computing industry. A “shift-left” strategy in the software development process integrates security controls and practices into every phase of the software development. With DevSecOps integrated into the CI/CD pipeline, this also brings automation into secure code reviews and security testing. Use of automated tools for detection, remediation of vulnerabilities in open-source software and detection, and management of secure posture provides an operator with quick detection and resolution of anomalies in the network.

O-RAN Alliance's architecture for RAN is built on the secure foundation of zero trust where network elements mutually authenticate with each other in order to communicate. All communication between them is transported over a secure interface per industry best practices specified by O-RAN Alliance's security specifications. While standards are still evolving, the Open RAN pioneers and ecosystem vendors like AltioStar, Mavenir, Fujitsu and Red Hat, as well as early adopters like Rakuten, Vodafone, Telefonica, NTT Docomo and DISH have ensured that all the interfaces are secured using certificate based security.

Every network element in the Open RAN network undergoes platform hardening as per 3GPP's security assurance specifications and other well-known cloud computing industry benchmarks such as CIS. This protects the network from an attacker gaining unauthorized access and subjecting the network to Denial-Of-Service (DOS) attacks or gaining illegal access.

In summary, open, standardized interfaces remove vulnerabilities or risk that comes with proprietary and potentially untrusted implementation and provides an operator full visibility and control over the cloud environment and network in general.



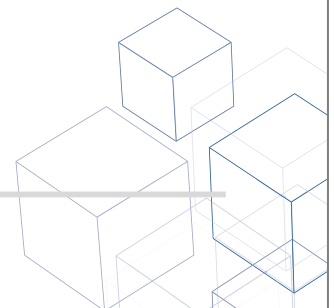
Appendix

References

- [1] 3GPP TS 38.401: NG-RAN; Architecture description
- [2] 3GPP TS 38.473: NG-RAN; F1 Application Protocol (F1AP)
- [3] O-RAN Architecture Description (O-RAN.WG1.O-RAN-Architecture-Description)
- [4] 3GPP TS 33.501: Security architecture and procedures for 5G system (Release 16)
- [5] NIST Special Publication 800-207: Zero Trust Architecture
- [6] O-RAN Architecture Description Chapter X – O-RAN Security
- [7] O-RAN Control, User and Synchronization Plane Specification (O-RAN WG4.CUS)
- [8] O-RAN Management Plane Specification (O-RAN.WG4.MP)
- [9] NIST Special Publication 800-190: Application Container Security Guide
- [10] 3GPP TS 33.511: Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
- [11] CIS benchmarks: <https://www.cisecurity.org/cis-benchmarks/>

Acronyms

3GPP	3rd Generation Partnership Project	OCI	Open Container Initiative
5G	5th Generation	O-CU	O-RAN Central Unit
CA	Certification Authority	O-DU	O-RAN Distributed Unit
CI/CD	Continuous Integration/Continuous Delivery	O-RAN	Open Radio Access Network
CIS	Center for Internet Security	O-RU	O-RAN Radio Unit
CMP	Certificate Management Protocol	PDCP	Packet Data Convergence Protocol
CNF	Cloud native Network Function	PNF	Physical Network Function
CP	Control Plane	RAN	Radio Access Network
CPRI	Common Public Radio Interface	RBAC	Role Based Access Control
CRI-O	Container Runtime Interface for OCI compatible runtimes	RIC	Radio Intelligent Controller
CRMT	Core Root of Trust Measurement	RLC	Radio Link Control
CSP	Cloud Service Provider	RT-RIC	Real-Time Radio Intelligent Controller
CU	Central Unit	RRM	Radio Resource Management
CUS	Control, User & Synchronization	RRU	Remote Radio Unit
DOS	Denial of Service	SAST	Static Application Security Testing
DDOS	Distributed Denial of Service	SCRM	Supply Chain Risk Management
DTLS	Datagram Transport Layer Security	SDAP	Service Data Adaptation Protocol
DU	Distributed Unit	SDLC	Software Development Life Cycle
EST	Enrollment over Secure Transport	SIEM	Security Information and Event Management
FIPS	Federal Information Processing Standards	SLA	Service Level Agreement
GSMA	Global System for Mobile Communications Association	SMO	Service Management and Orchestration
HSM	Hardware Security Module	SSH	Secure Shell
ICAM	Identity, Credential and Access Management	STG	Security Task Group
LLS	Lower Layer Split	SUCI	Subscription Concealed Identifier
LUKS	Linux Unified Key Setup	TCO	Total Cost of Ownership
MAC	Mandatory Access Control	TLS	Transport Layer Security
MEC	Multi-access Edge Computing	TPM	Trusted Platform Module
MITM	Man-in-the-Middle	UE	User Equipment
NDS	Network Domain Security	UP	User Plane
NESAS	Network Equipment Security Assurance Scheme	VNF	Virtualized Network Function
NF	Network Function	ZTA	Zero Trust Architecture
NIST	National Institute of Standards and Technology		
NR	New Radio		
NR-RIC	Near Real Time RIC		



ATTACHMENT 5

Mavenir, *Open RAN: Mature and Ready for Deployment* (describing power performance and efficiency)



OpenRAN: Mature and Ready for Deployment

February 2021



[mavenir.com](https://www.mavenir.com)

Open RAN – Mature and Ready for deployment

Introduction

While the Open RAN momentum is continuously growing, most recently bolstered by the MoU among EU operators¹, traditional vendors have trouble deciding whether Open RAN is a serious threat or should be part of their R&D investment as they commit to Open RAN as the future architecture. At every stage, traditional vendors have raised concerns on aspects such as performance, security, and integration costs, creating fear, uncertainty and doubt among operators who are looking at options to build and evolve their networks.

It is worth restating that Open RAN is about having Open and Interoperable Interfaces for product nodes to allow multiple vendors to produce interoperable products and widen the supply chain. Open RAN does not describe or mandate how a node be implemented whether it be in virtualized software or dedicated custom hardware.

This white paper article focuses on the following Open RAN architecture aspects:

1. Security Aspects
2. Power savings with Open RAN based architectures
3. Cost optimization with COTS
4. Cloud benefits with Open APIs – Automation & Scaling
5. Performance improvement with RIC and AI/ML
6. Mature eco-system
7. Faster Time to market
8. Innovation

¹ <https://www.totaltele.com/508561/TIM-joins-the-party-for-European-Open-RAN>

1. Security Aspects

Security aspects of Open RAN architecture have been already addressed in previous white papers².

2. Power savings with Open RAN based architectures

Statements have been made that Open RAN deployments consume up to 40% more power than current deployments. However, when comparing equivalent configurations of D-RAN/C-RAN with Open RAN, Open RAN actually provides power savings through the use of inherent architecture changes described in the O-RAN Alliance fronthaul 7.2 specification that focus on reducing transmission bandwidth when there is lower traffic and power saving features such as use of Section Type 0 for putting radio in low power mode when idle.

a) Fronthaul power savings

On an equivalent basis, power saving is achieved through following aspects: -

- The speed of the O-RAN interface is a fraction of the interface speed when compared to CPRI and has a direct effect in lowering power consumption . The transmission bandwidth savings can even be greater than 4X for 4T4R radios using features available in the specification such as fronthaul compression and sending frequency domain samples as available from the O-RAN specification and can be much more for massive MIMO if layer information is sent instead of antennas with precoding done in the radios. The reduction in transmission bandwidth also has a direct benefit on lowering the power consumption of network interface cards (NIC), CPU packet processing and power savings through the complete fronthaul network.

² <https://mavenir.com/resources/openran-architecture-provides-path-to-secure-open-networks/>

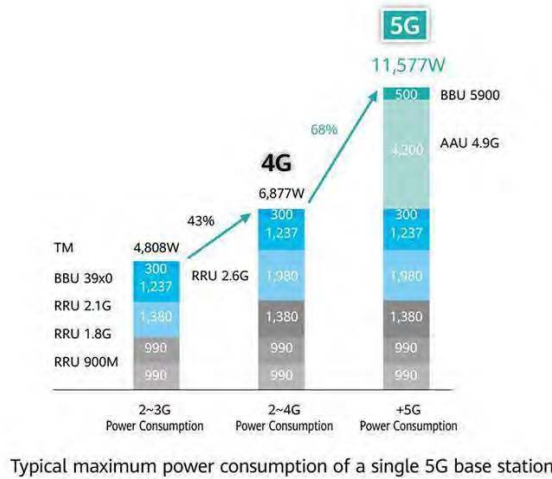


- As designed in the O-RAN front haul interface specification, the used transmission bandwidth is proportional to the user bandwidth. If there is zero traffic, there is minimal front haul interface traffic allowing the power consumption to be minimized.
- With no traffic, the DU draws minimal power and uses minimal CPU core resources due to minimal traffic. This allows the DU to be overprovisioned supporting multiple RRUs per DU eliminating dedicated DU's per radio given step functions in power savings.

b) RF power savings

The RF dominates the power consumption at a cell site for 5G as shown in the figure below from Huawei. Open RAN interfaces do not impact the radio (RF) power consumption. The RF power consumption is not impacted by the interface since the radio only performs time domain processing and uses optimized fronthaul. The Open RAN ecosystem is growing through white box radio developments such as Evenstar with Facebook, MTI and Mavenir. With the removal of margin stacking, licenses structure and the saving in power consumption through RF device innovation, the radio cost can come down substantially. There have been multiple announcements by Analog Devices, Maxlinear, Fujitsu, MTI and others related to innovative DPD/CFR techniques. Such innovation will be further strengthened by the entry of multiple new players in the Open RAN ecosystem. The power savings of radios with Open RAN based split 7 architectures has also been demonstrated by NEC in their Rakuten deployment³.

³ https://www.nec.com/en/press/202003/global_20200324_02.html



Source: Huawei⁴

c) RAN software power savings.

As the disaggregated RAN compute resources move to data centers, the power efficiency can take advantage of the global data center power optimization trends. The data center power consumption has increased by 6% since 2010 but at same time the amount of compute in the data center has increased by 550%⁴. With centralized baseband processing in the cloud, it is much easier to pool resources taking into account the workload variations across cell sites and time of day and implement usage-based power savings that can be adjusted dynamically. A NGMN study in Europe shows that 80% of a wireless network carry only 20% of the traffic.⁵ and pooling across sites could potentially reduce DU/CU capacity requirements with significant compute and power savings. With scalability and demand-based usage, processors (CPUs or GPUs) that are processing radio software can also run other applications during non-peak times. This is

⁴ <https://www.datacenters.com/news/data-center-power-optimization-increase-efficiency-with-a-data-center-audit>

⁵ https://www.ngmn.org/wp-content/uploads/NGMN_RAN_EV_D2_Further_Study_on_Critical_C-RAN_Technologies_v1.0.pdf

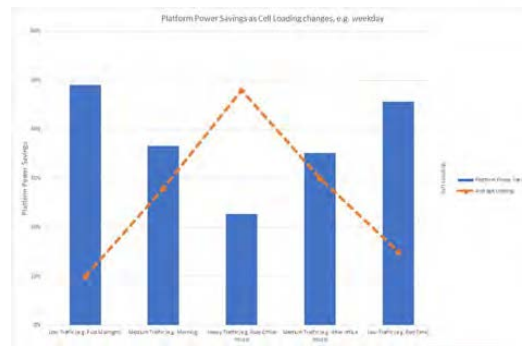
not possible with proprietary baseband systems using dedicated, non-reusable hardware.



Source: NGMN⁵

d) Platform Power Savings with load

Moving RAN to the cloud using open interfaces offers potential reduction of electricity cost, as the RAN processing can now be shared among cell sites. In densely deployed networks, as in city centers, the network traffic load can fluctuate very much during the day, with significant periods of minimal traffic at certain cell sites for extended periods. There are also many short gaps in the data transmissions even during highly loaded times. Modelling the cell load profile over a 24-hour period over different types of cells, demonstrates that power savings in the range of 30-55% can be achieved.

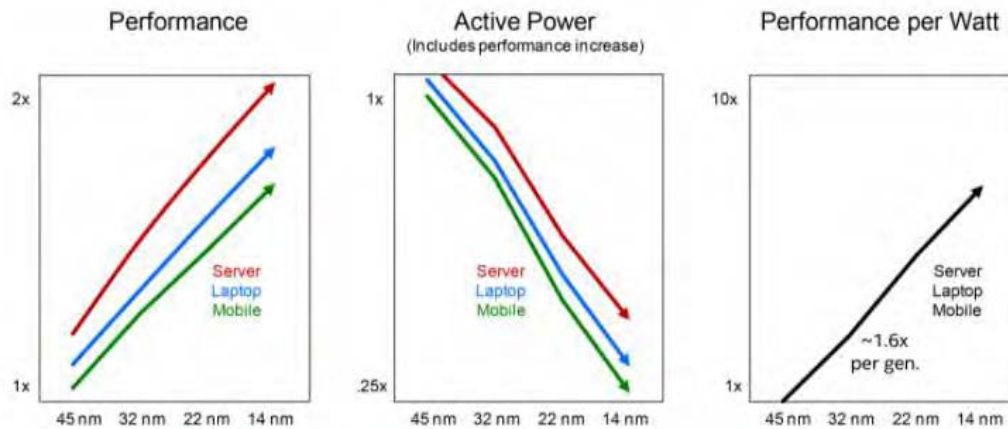


Elastic Power Savings

Advanced measurements using AI/ML can be performed to predict traffic patterns, traffic load, and end-user needs, from network level across nodes down to subframe levels with a cell. Based on this data, RAN compute and radio equipment can be dynamically activated to achieve the lowest possible energy consumption with maintained network performance. The dynamic compute provisioning optimizes utilization of silicon and prevents over-provisioning of resources. This results in reduction in power and energy consumption compared to traditional RAN architecture, improves scalability, and consequentially lowers the TCO.

This consolidation also enables telco operators to take advantage of existing compute and storage infrastructure offered by cloud providers, instead of incurring all such costs in-house. A public cloud hosted deployment will significantly reduce the investment burden on telco operators.

When looking at processor roadmaps, power efficiency and capacity is improved with every generation of the processor technology providing performance improvements as the transistor feature size continues to shrink. Also, further optimizations are possible for dynamic power management using processor BIOS and power settings to control the voltage and frequency of the processor based on the network configuration and usage. The figure below shows roughly a 1.6X improvement in performance per watt every processor generation.



New technology generations provide improved performance and/or reduced power, but the key benefit is improved performance per watt

Source: Intel

d) Accelerator power savings

To restate, just because RAN is now open – dedicated hardware can still be used for specialized functions for performance and power saving improvements. – **Open RAN simply implies interfaces are open.** Though the preference is for COTS hardware from a reuse preference, dedicated (e)ASICs, FPGAs, GPUs, and other such commercially open accelerators, are perfectly acceptable solutions to provide hardware function acceleration and power savings in the context of open RAN. The performance and power optimizations on these accelerators are also rapidly improving with every generation as they address the telecom market, and they are being made more generic to support a wider variety of applications with the same hardware.

3. Cost optimization with cloud and COTS

1. Operators throw away proprietary systems from traditional vendors every few years and are unable to use these proprietary radio systems for any other application. In the



last 25 years, as we have gone from 2G to 5G, legacy telecom vendors have not changed and keep building proprietary systems while the whole world around telecom operators have embraced open systems and cloud.

2. Proprietary radio implementation using closed interfaces support “rip & replace” strategies as the entire solution has to be fully replaced with every vendor, every technology change or feature requirement.
3. Utilizing Open RAN based solutions in a web scale way enables operators to leverage general purpose off the shelf computing hardware.
4. Centralized pooling for RAN will deliver commercial rate benefits in addition to the power consumption and capacity benefits. Usually, large data centers qualify for preferential rates in many parts of the world vs. individual cell sites. There are also other opportunities for alternative energy sources to be applied due to scale and easier logistics.
5. If carriers adopt cloud technologies now, they will build not only 4G and 5G networks but will be 6G ready as there will be reuse with their current investments. There is now an incentive for open silicon vendors to apply their technology to telecom applications.
6. Accelerator chips that are used for gaming, life sciences, algorithms can be used for telecom applications without sacrificing interoperability across Open Interfaces. Open RAN has standardized accelerator APIs so that various forms of acceleration can work with COTS hardware. The cost for building these systems will come down significantly due to a wider customer base for such accelerators.

4. Cloud benefits with Open APIs – Automation & Scaling

1. With 4G/5G, there are a wide variety of use cases that need to be supported with flexible requirements on data rates, latencies, and functionality. Disaggregated RAN enables open API-based cloud implementations, which allow for scaling with the same software and hardware architecture to support different use cases.



2. With cloud technology adoption in an open RAN architecture with a common application platform (Open RAN software to Packet Core to IMS), one can make use of the entire automation and CI/CD processes across the entire E2E network including the radio.
3. Having an open disaggregated RAN architecture with cloud native implementations allows the use of different types of data centers that can be owned by operators or by hyperscale providers to host these RAN software workloads. These data centers could range from edge data centers such as AWS Outpost or Google Anthos to public and hybrid clouds and the operator has flexibility in deployment based on the use cases and transport availability and pay-as-you-grow models for scalability. For e.g., to support low latency application if the Operator does not have own data center, users could be serviced using radio software running on Edge data center from a hyperscale cloud provider partner.
4. RAN deployment times and software upgrade times can benefit from innovation in IT industry moving from hours to minutes and new features can be added in days instead of months [see chart below called “End2End Network Automation” from a commercial Open RAN deployment in Rakuten which highlights benefits in E2E automation across customer activation, cell site deployment, new feature deployment and network availability]
5. By adding radio as an additional application in the cloud, network data obtained from multiple sources in the cloud (including the RAN, Core, IMS etc.) can be now collected in a common datalake using a standardized and open observability framework interface. AI/ML based analytics can then be used to process the data from the datalake and obtain network wide insights and implement network wide performance optimization.

E2E Network Automation

Rakuten Mobile operates like no other existing telco in the world



Source: Rakuten

5. Performance improvement with RIC and AI/ML

1. Several operators such as Vodafone and Verizon have mentioned the Open RAN and virtualized solutions are already meeting or even exceeding their KPI expectations.
 - a. From Vodafone CEO⁶: *"We have had trials taking commercial traffic for about a year now," he said. "It is a 2G, 3G and 4G trial and it is live and the KPIs [key performance indicators] are really good and **in some cases better than the incumbent.**"*
 - b. Operators such as Verizon have already adopted vRAN and are now aligning with Open RAN as well
2. One of the performance benefits provided by Open RAN is the ability to add artificial intelligence and machine learning (AI/ML) based network optimizations with a standardized API so that the open community can contribute to applications to optimize the network without having to provide the entire solution. This functionality is being enabled by the O-RAN alliance with the Real time Intelligent Controller specifications.

⁶ <https://www.lightreading.com/open-ran/vodafone-ceo-read-targets-urban-open-ran-in-2022/d/d-id/762704>



RIC enables mobility optimizations and provides greater control of the RAN to the operator enabling policy settings to tune the network.

3. Centralization of RAN CU/DU processing enables feature optimizations that can use information across cell sites for the RAN processing at a centralized location and provide improved spectral efficiency and latency optimizations such as interference management with COMP, multi-cell scheduling and handover optimizations between cells connected to same CU/DU.

6. Mature eco-system

1. The standardization aspects for Open RAN O-RAN started in 2017 and the O-RAN specifications are now mature in their fifth revision published with 237 mobile operators⁷ and network equipment providers who are now part of the O-RAN ecosystem. There are O-RAN compliant products from multiple vendors, and this has been deployed and validated in commercial networks such as Rakuten, Vodafone, Telefonica, DT, TIM, Orange to name a few and is being deployed by many other operators worldwide.
2. The OpenRAN Policy Coalition (ORPC) as of February 2021, has over 60 members⁸. Coalition members represent a cross-section of the wireless communications industry globally, ranging from network operators to network solutions providers, systems integrators, cloud providers, edge device manufacturers, and more. The Coalition presently consists of the following members: Airspan, AltioStar, American Tower, Analog Devices, ARM, AT&T, AWS, Benetel, Bharti Airtel, Broadcom, Ciena, Cisco, Cohere Technologies, CommScope, Crown Castle, DeepSig, Dell Technologies, Deutsche Telekom, DISH Network, Facebook, Fujitsu, GigaTera Communications, Google, Hewlett Packard Enterprise, IBM, Inseego, Intel, JMA Wireless, Juniper Networks, Ligado Networks, Marvell, Mavenir, Microsoft, NEC Corporation, NewEdge Signal Solutions,

⁷ <https://techblog.comsoc.org/category/o-ran/>



Nokia, NTT, Nvidia, Oracle, Palo Alto Networks, Parallel Wireless, Pivotal Commware, Qualcomm, Quanta Cloud Technology, Radisys, Rakuten Mobile, Reliance Jio, Rift, Robin, Samsung Electronics America, STL Tech, Telefónica, Texas Instruments, U.S. Cellular, US Ignite, Verizon, VMWare, Vodafone, World Wide Technology, XCOM-Labs, and Xilinx.

7. Faster Time to market

1. Open RAN is both time and cost efficient in terms of deployment. Operators do not have to wait for customized hardware and set of features from a single vendor to start their deployment. Operators can go with whichever vendor(s) who is/are ready with the features they need and enable competition between vendors to serve their deployment needs in a timely manner.
2. As the different parts of the Open RAN ecosystem have built up (hardware vendors, chipset providers, software players), the various vendors supporting the ecosystem have also come together testing interoperability. So, there are no inherent blockers in Open RAN technology itself.
3. Open RAN enables virtualization, which implies faster development and innovation using open-source tools. This enables operators to ensure multiple sources of supply and not be dependent on single source as closed systems are today.
4. With Open RAN deployments and container-based virtualization of applications, operators can use automation frameworks already widely used in the IT industry such as CI/CD processes for all applications, reducing deployment times and software upgrade times from hours to minutes.

8. Innovation

Lack of innovation and closed systems has put the whole industry in a bad economic situation. Operators spend billions to buy spectrum, spend billions to build networks and then spend billions to give phones free to people for them to stay on those



networks. There is no money left to do anything innovative. Companies like Zoom, Twilio, Snap chat and many others make money running on these networks.

Open RAN also enables open-source eco-system for development. A comparison can be made with Linux and Microsoft, when it was mentioned that open-source software will make all applications on that platform open source and unusable, which turned out to be false⁸. **The key is Open Interfaces.** Open RAN, by enabling open APIs, enables innovation, while allowing vendors to differentiate within the applications and functionality provided by their hardware and software.

1. Having an Open RAN architecture now enables multiple vendors and operators to co-operate, contribute and innovate on new technologies as the industry moves towards 6G.

For more information, visit www.mavenir.com

⁸ https://www.theregister.com/2001/06/02/ballmer_linux_is_a_cancer/